Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Infoblox DNSone DHCP Failover or High Availability in an Avaya Communication Manager IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Infoblox DNSone for DHCP Failover as well as the procedure for configuring Infoblox DNSone for High Availability in an Avaya Communication Manager IP Telephony Infrastructure. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

©2006 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes focus on the steps required for configuring Infoblox DNSone DHCP Failover or High Availability in an Avaya Communication Manager IP Telephony environment. For information on how to configure Infoblox DNSone to deliver DHCP and TFTP services in an Avaya IP Telephony environment, please refer to the Application Notes in references [4], [5], and [6].

The Infoblox DNSone delivers integrated DNS, DHCP and TFTP services for Infoblox network identity appliances. It may be used as an integrated DNS/DHCP/TFTP server, external authoritative name server, external secondary name server, name server forwarder, caching-only name server, or DHCP-only server. Configuration of the DNSone is done through a web-based graphical user interface. The DNSone also provides security and reliability features. It minimizes unauthorized access by blocking unnecessary ports and not providing general user accounts (multiple administrative accounts are allowed). For increased reliability, two DNSone appliances may be deployed in a DHCP Failover or High Availability configuration.

A DHCP Failover configuration in the DNSone allows either a primary or secondary DHCP server to assume control of DHCP services in case either of the two servers fails. A secondary DHCP server assumes control if the primary fails, and the primary expands its control if the secondary fails, even though both may be leasing IP addresses to DHCP clients. DNSone's DHCP failover configuration also supports lightweight load balancing. Please refer to the Infoblox product documentation in reference [7] for further information and requirements.

A High Availability configuration for the DNSone consists of two physical DNSone appliances that are linked to perform as a single virtual device. In this configuration, one device is the active node and the other is the passive node. One appliance is actively functioning as the master while the other appliance is a passive backup. The passive DNSone maintains the synchronization of its settings and run-time objects with the active DNSone so that it can seamlessly take over if a failover occurs.

The tested configurations are shown in **Figure 1** and **Figure 2**.

The configuration in **Figure 1** shows a network consisting of the Avaya S8300 Media Server with G700 Media Gateway, Avaya 4600 Series IP Telephones, and two Infoblox DNSone appliances configured for DHCP Failover connected to an Avaya C363T-PWR Stackable Switch. The Avaya IP Telephones registered to the Avaya S8300 Media Server.

©2006 Avaya Inc. All Rights Reserved.

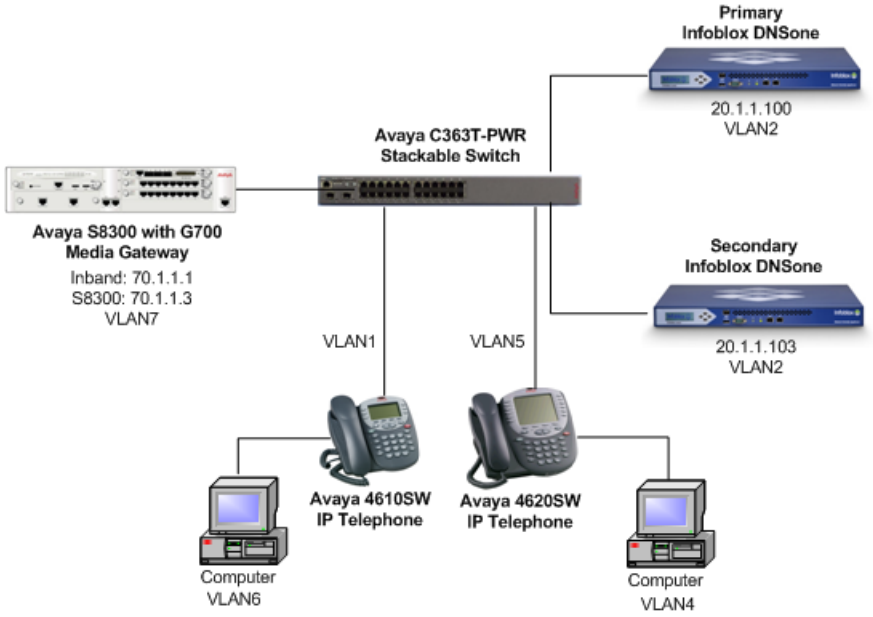


Figure 1 – Sample DHCP Failover Network Configuration Diagram

The configuration in **Figure 2** shows a network consisting of the Avaya S8300 Media Server with G700 Media Gateway, Avaya 4600 Series IP Telephones, and two Infoblox DNSone appliances configured as a High Availability pair connected to an Avaya C363T-PWR Stackable Switch. The Avaya IP Telephones registered to the Avaya S8300 Media Server.

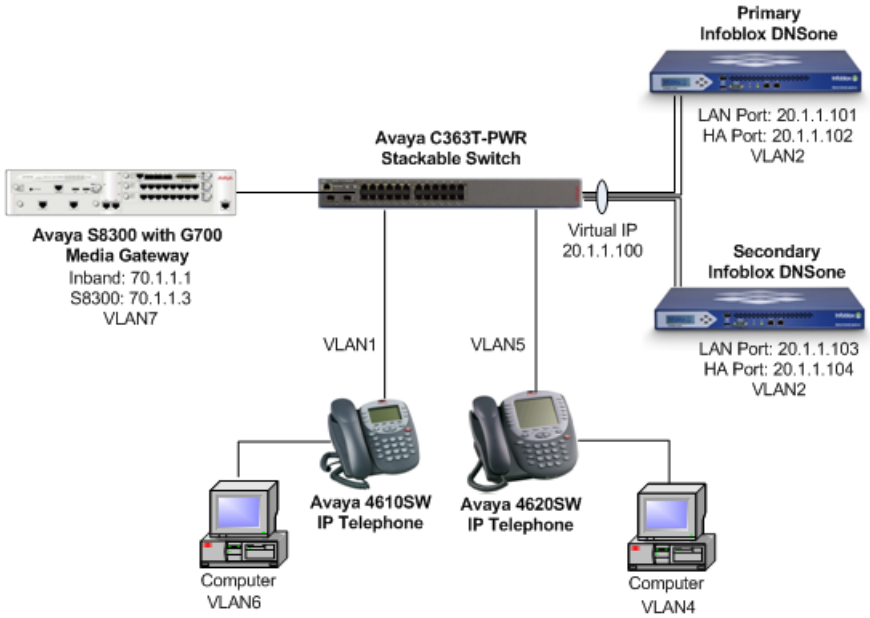


Figure 2 – Sample High Availability Network Configuration Diagram

©2006 Avaya Inc. All Rights Reserved.

Table 1 shows the DHCP Option 176 string settings the Infoblox DNSone DHCP server must provide for the Avaya 4600 IP Telephones to register with Avaya Communication Manager in the sample configurations.

VLAN	Scope	Option 3 Router	Option 176 String (do not insert blanks in string)
VLAN1	10.1.1.0/24	10.1.1.254	MCIPADD=70.1.1.3,MCPORT=1719,TFTPSRVR=20.1.1.100
VLAN4	40.1.1.0/24	40.1.1.254	L2Q=1,L2QVLAN=5
VLAN5	50.1.1.0/24	50.1.1.254	MCIPADD=70.1.1.3,MCPORT=1719,TFTPDIR=/040405/,TFTPSRVR=20.1.1.100
VLAN6	60.1.1.0/24	60.1.1.254	L2Q=1,L2QVLAN=1

Table 1 – DHCP Option 176 by VLAN Information

The Option 176 string for VLAN1 and VLAN5 differs slightly to illustrate the use of parameter TFTPDIR. VLAN1 used files from the DNSone TFTP root directory whereas VLAN5 used files from the subdirectory assigned to the TFTPDIR parameter in the Option 176 string. This was done to verify that the DNSone TFTP server could be used to download files from different subdirectories.

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configurations provided:

Equipment	Software/Firmware
Avaya S8300 Media Server in a G700 Media Gateway	3.01 (R013x.00.1.346.0)
Avaya C363T-PWR Stackable Switch	4.3.12
Avaya 4600 Series IP Telephones (4610SW, 4620SW)	2.3
Infoblox DNSone	3.2

Table 2 – Equipment and Software / Firmware Versions Validated

3. Reset the Avaya IP Telephones

The information provided in this section describes the steps required to reset the Avaya 4600 IP Telephones to factory defaults.

For all other provisioning information, please refer to the Avaya 4600 IP Telephone product documentation in reference [1].

Step	Description
1.	With the Avaya 4600 IP Telephone powered on and on-hook (idle), press the **MUTE** button and then press the following keys in sequence on the dial pad: **73738#** (**RESET#**).
2.	When prompted to **Reset Values?**, press the **#** key. This will reset any previously assigned values. When prompted to **Restart Phone?**, press the **#** key.
3.	Repeat Steps 1 – 2 for each Avaya 4600 IP Telephone depicted in **Figure 1**.

©2006 Avaya Inc. All Rights Reserved.

4. Configure the Avaya C363T-PWR Stackable Switch

The configuration information provided in this section describes the steps required to enable DHCP relay on the Avaya C363T-PWR Stackable Switch.

For all other provisioning information, please refer to the Avaya C363T-PWR Stackable Switch product documentation in references [2] and [3].

Step	Description
1.	Log into the C363T-PWR with the appropriate credentials via the console port.

2.	Enter into router configuration mode:
	`C360-1(super)# **configure**`
	`C360-1(configure)#`
	
	`C360-1(configure)# **session router**`
	`Router-1(configure)#`

3.	Enable DHCP relay: `Router-1(configure)# **ip bootp-dhcp relay**`
	For Infoblox DNSone DHCP Failover, execute steps 4 and 5.

4.	For each interface that connects to DHCP clients, specify the IP address of the DHCP server that will handle the DHCP requests received on the interface:
	`Router-1(configure)# **interface vlan1**`
	`Done!`
	`Router-1(config-if:vlan1)# **ip bootp-dhcp server 20.1.1.100**`
	`Done!`
	`Router-1(config-if:vlan1)# **ip bootp-dhcp server 20.1.1.103**`
	`Done!`
	`Router-1(config-if:vlan1)# **exit**`
	`Done!`

5.	Repeat Step 4 for the remaining VLANs that have DHCP clients in **Table 1**. This completes the configuration of the C363T-PWR for DNSone DHCP Failover.
	For Infoblox DNSone High Availability, execute steps 6 and 7.

6.	For each interface that connects to DHCP clients, specify the IP address of the DHCP server that will handle the DHCP requests received on the interface:
	`Router-1(configure)# **interface vlan1**`
	`Done!`
	`Router-1(config-if:vlan1)# **ip bootp-dhcp server 20.1.1.100**`
	`Done!`
	`Router-1(config-if:vlan1)# **exit**`
	`Done!`

7.	Repeat Step 6 for the remaining VLANs that have DHCP clients in **Table 1**. This completes the configuration of the C363T-PWR for DNSone High Availability.

5. Configure the Infoblox DNSone

The steps provided in this section are for configuring two Infoblox DNSone appliances for either DHCP Failover (Section 5.1) or High Availability (Section 5.2).

©2006 Avaya Inc. All Rights Reserved.

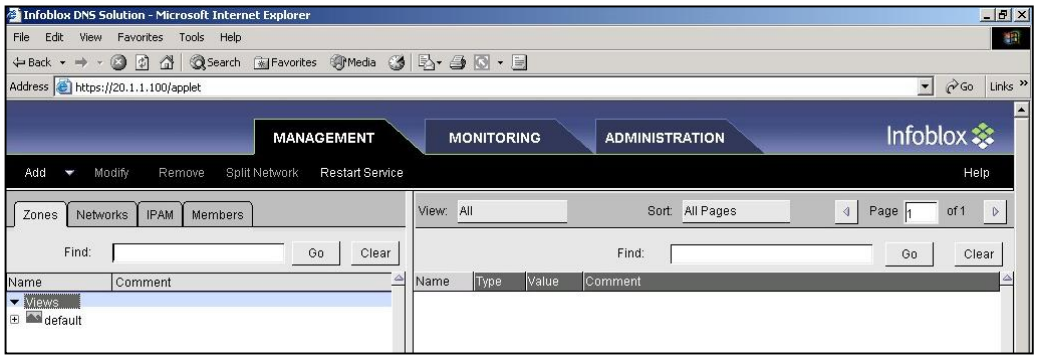
For all other provisioning information, please refer to the Infoblox DNSone product documentation in reference [7].

5.1. Configure DHCP Failover

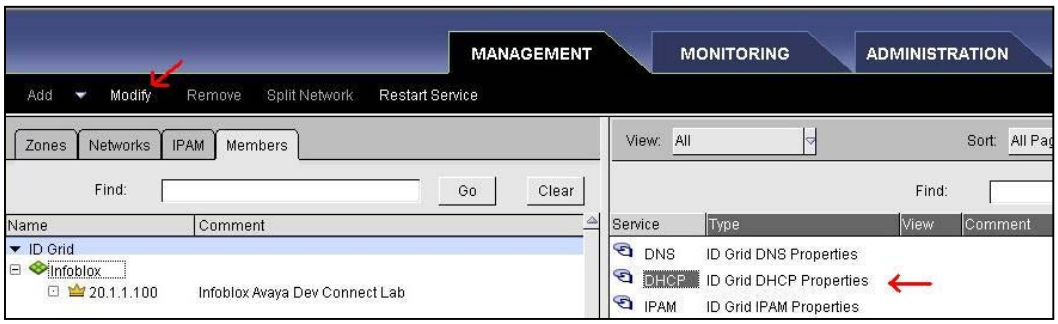
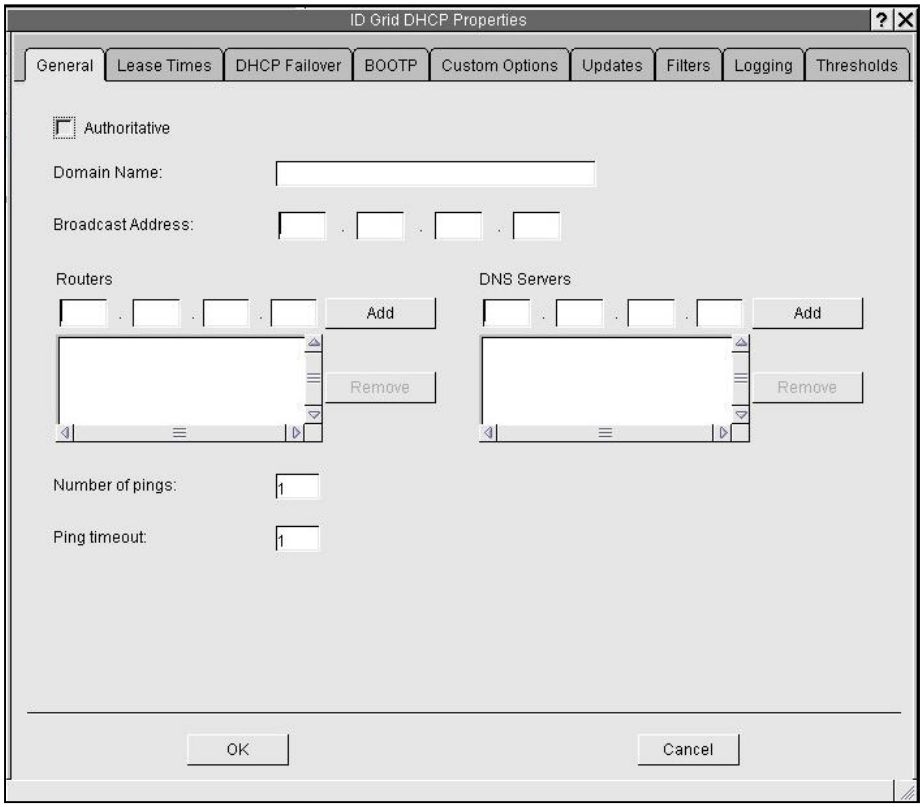
The instructions in this section assume:

- The Primary DNSone has already been configured with the appropriate network IP address, 20.1.1.100, via the console port.
- The Secondary DNSone has already been configured with the appropriate network IP address, 20.1.1.103, via the console port.
- Both DNSone's (Primary and Secondary) in **Figure 1** have been configured identically as per instructions provided in Sections 5.1 – 5.3 of the *Application Notes for Infoblox DNSone in an Avaya Communication Manager IP Telephony Infrastructure* in reference [4]. Both DNSone appliances have been initially configured with the same DHCP and TFTP configuration, including IP address ranges.

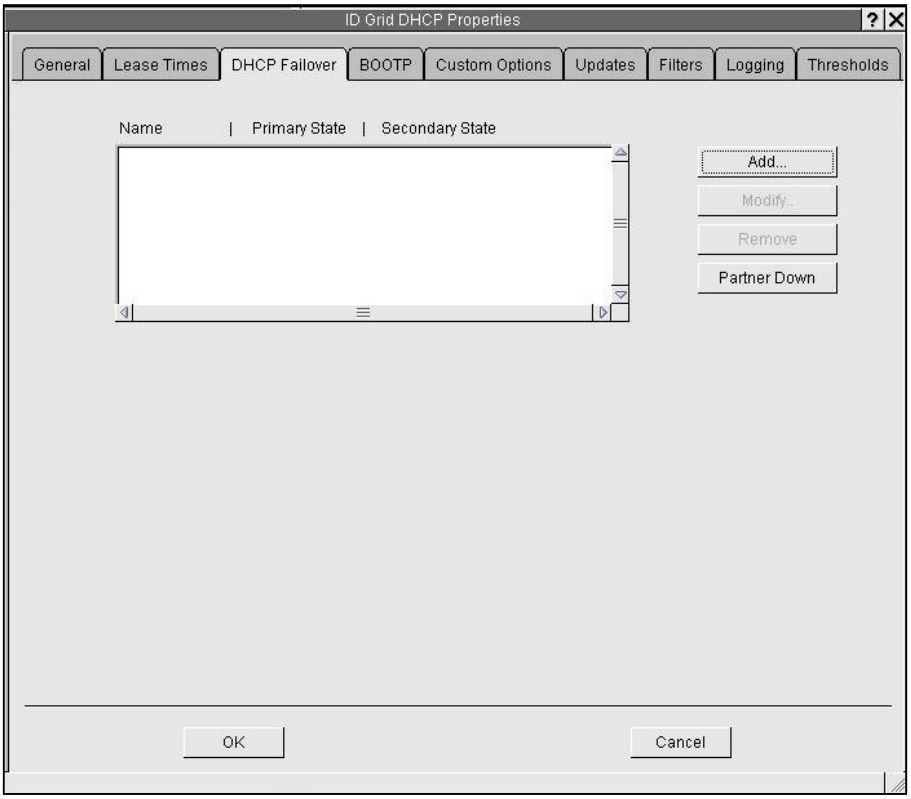
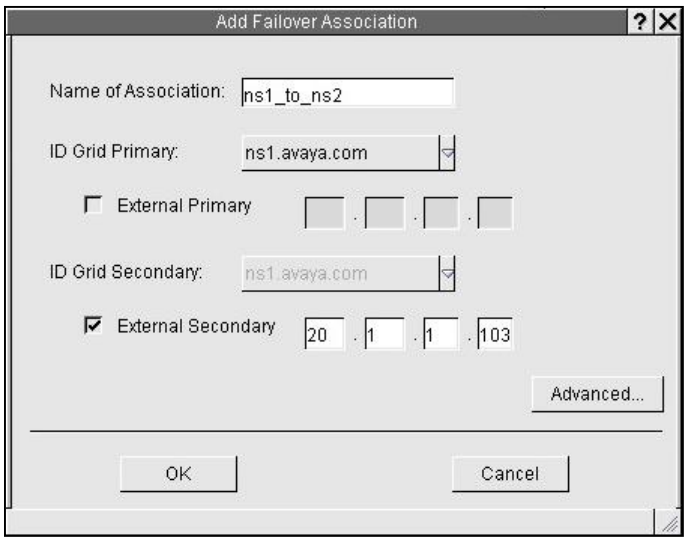
5.1.1. Configure Primary DNSone

Step	Description
1.	From a computer in the network, launch a browser and browse to https://20.1.1.100. Log into the Infoblox DNSone with the appropriate credentials (not shown).
2.	If a Warning – HTTPS popup (not shown) appears, click **Yes**.
3.	In the Infoblox DNS Solution page that appears, select the **Members** tab in the left pane. 

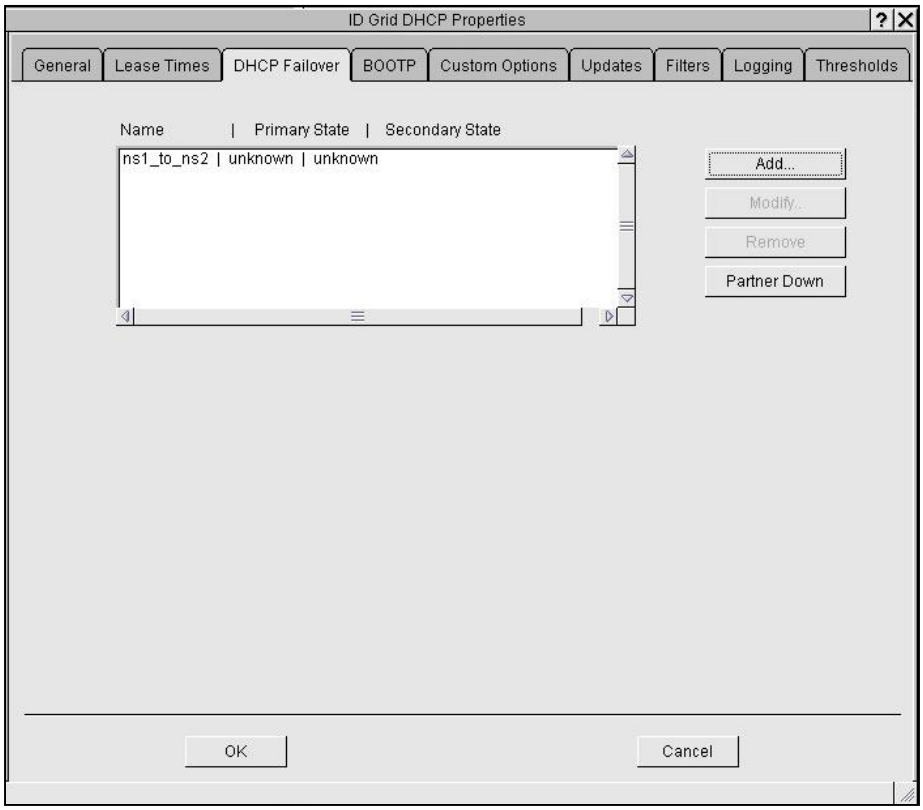
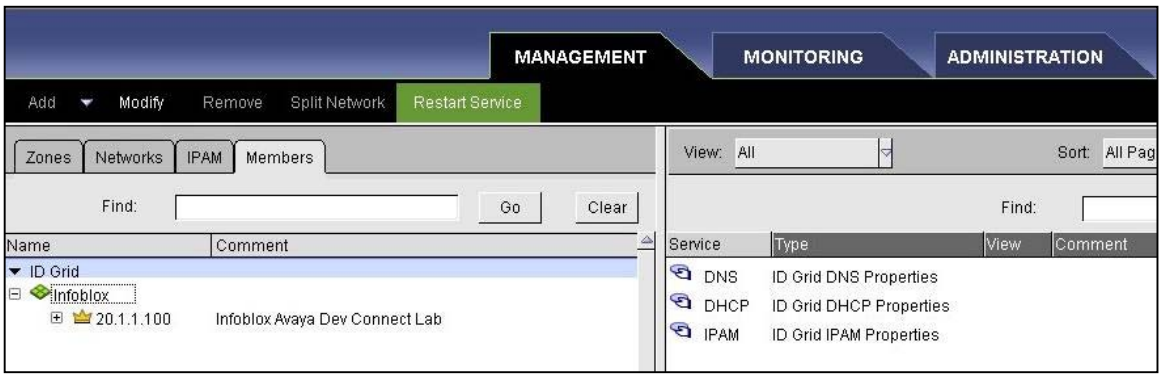
©2006 Avaya Inc. All Rights Reserved.

Step	Description
4.	In the Members page that appears, browse to **ID Grid → Infoblox** in the left hand pane, click or highlight the **DHCP** (ID Grid DHCP Properties) service on the right hand pane, then click **Modify** in the menu bar located above the Members tab. 
5.	In the ID Grid DHCP Properties popup that appears, select the **DHCP Failover** tab. 

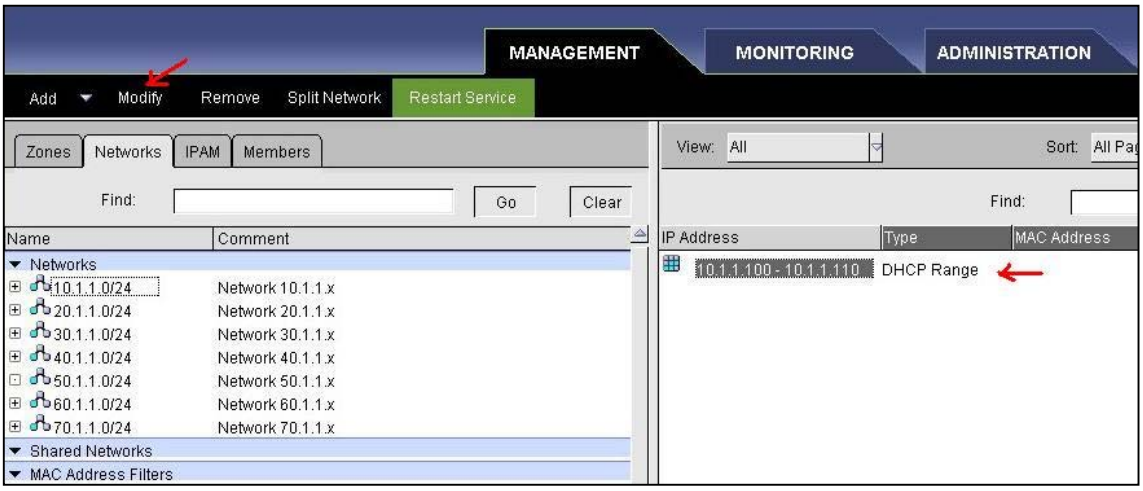
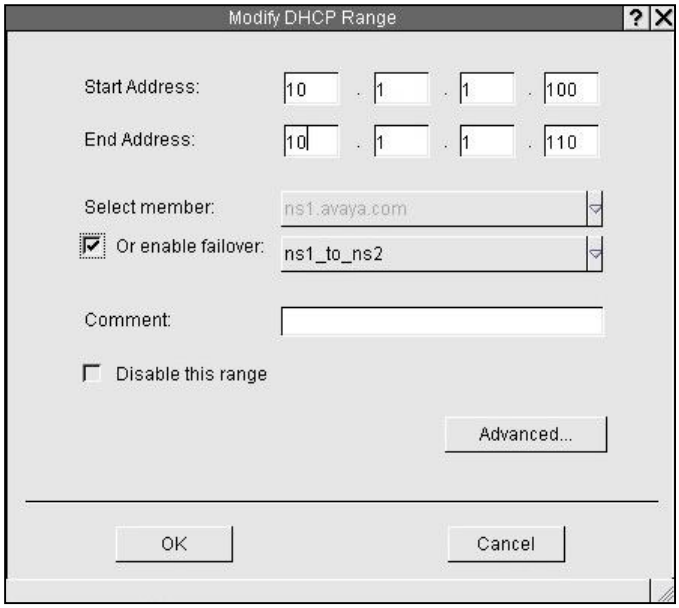
©2006 Avaya Inc. All Rights Reserved.

Step	Description
6.	In the DHCP Failover tab that appears, click **Add…** 
7.	In the Add Failover Association popup that appears, set **Name of Association** to the desired name, check **External Secondary** and enter the IP address of the Secondary DNSone for External Secondary. Click **OK**. 

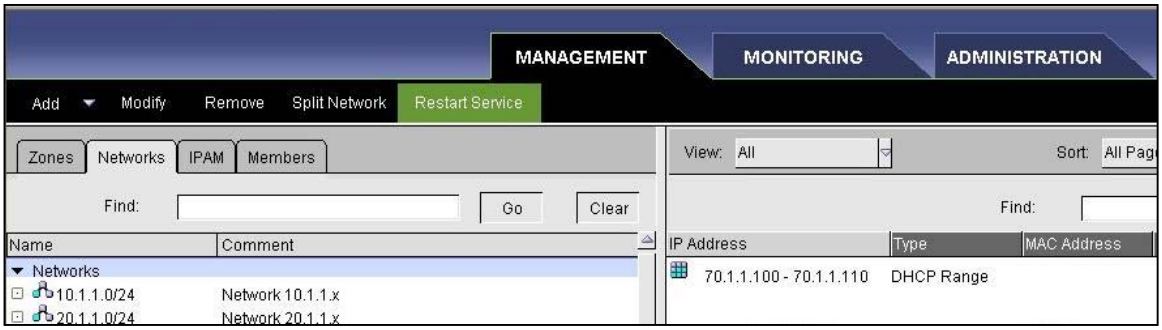
©2006 Avaya Inc. All Rights Reserved.

Step	Description
8.	In the DHCP Failover tab, click **OK**. 
9.	In the Members page that appears, select the **Networks** tab. 

©2006 Avaya Inc. All Rights Reserved.

Step	Description
10.	In the Networks page that appears, browse to **Networks → 10.1.1.0/24** in the left hand pane, click or highlight the **10.1.1.100 – 10.1.1.110** (DHCP Range) on the right hand pane then click **Modify** in the menu bar located above the Members tab. 
11.	In the Modify DHCP Range popup that appears, check **Or enable failover** and set the pull down list next to the field to the name set for ***Name of Association*** in Step 7. Click **OK**. 
12.	Repeat Steps 10 – 11 for each VLAN defined in **Table 1**. For the purposes of these Application Notes, all VLANs listed in **Table 1** were modified.

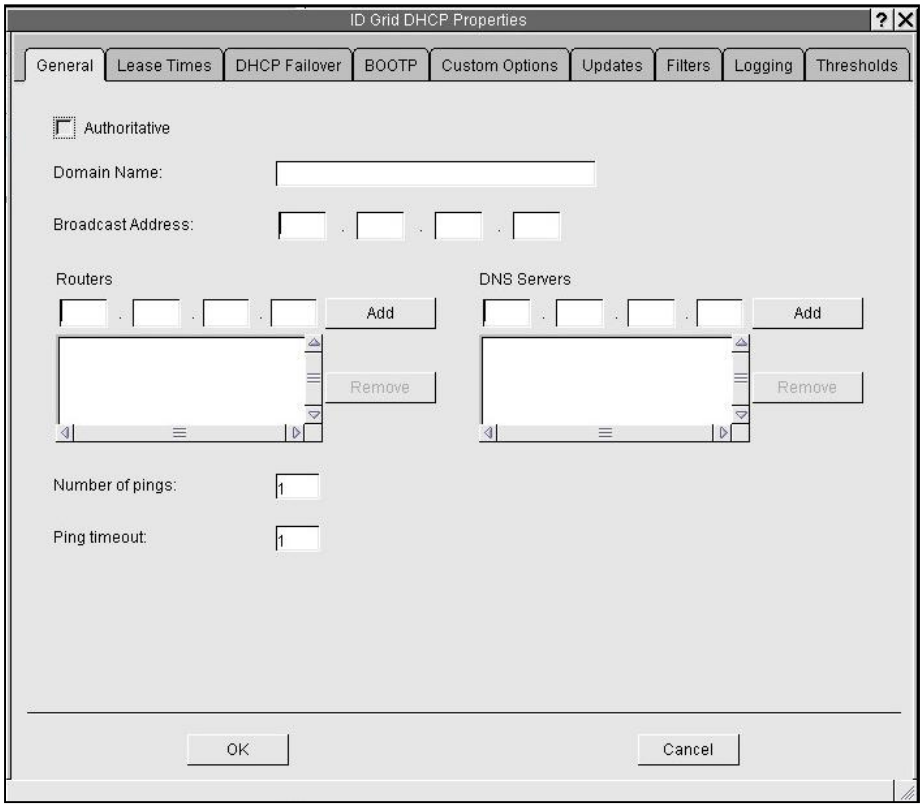
©2006 Avaya Inc. All Rights Reserved.

Step	Description
13.	Click **Restart Service**. 
14.	In the Restart Service popup that appears, select **Immediately** and click **OK**. This completes configuration of the Primary DNSone for DHCP Failover.

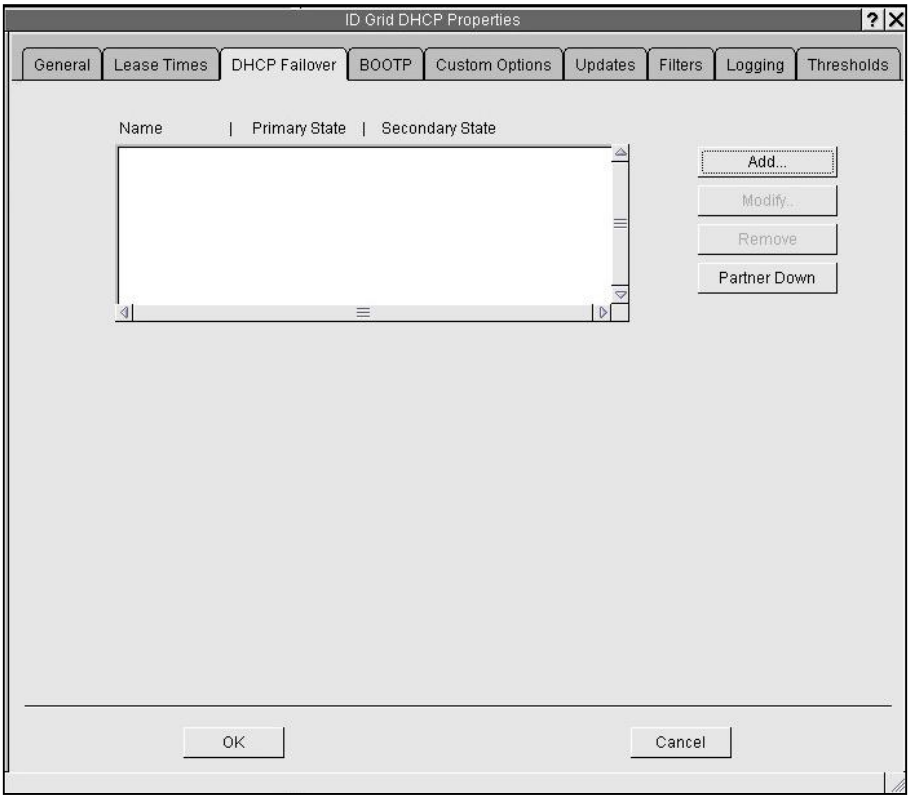
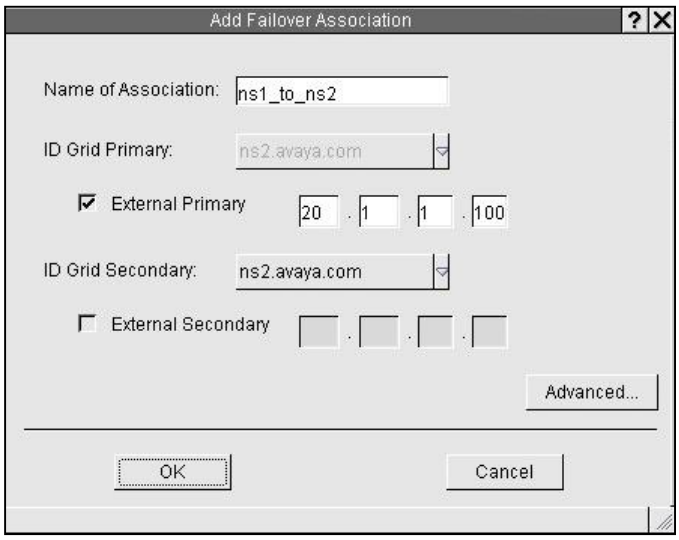
5.1.2. Configure Secondary DNSone

Step	Description
1.	From a computer in the network, launch a browser and browse to https://20.1.1.103. Log into the Infoblox DNSone with the appropriate credentials (not shown).
2.	If a Warning – HTTPS popup (not shown) appears, click **Yes**.
3.	In the Infoblox DNS Solution page that appears, select the **Members** tab in the left pane (not shown).

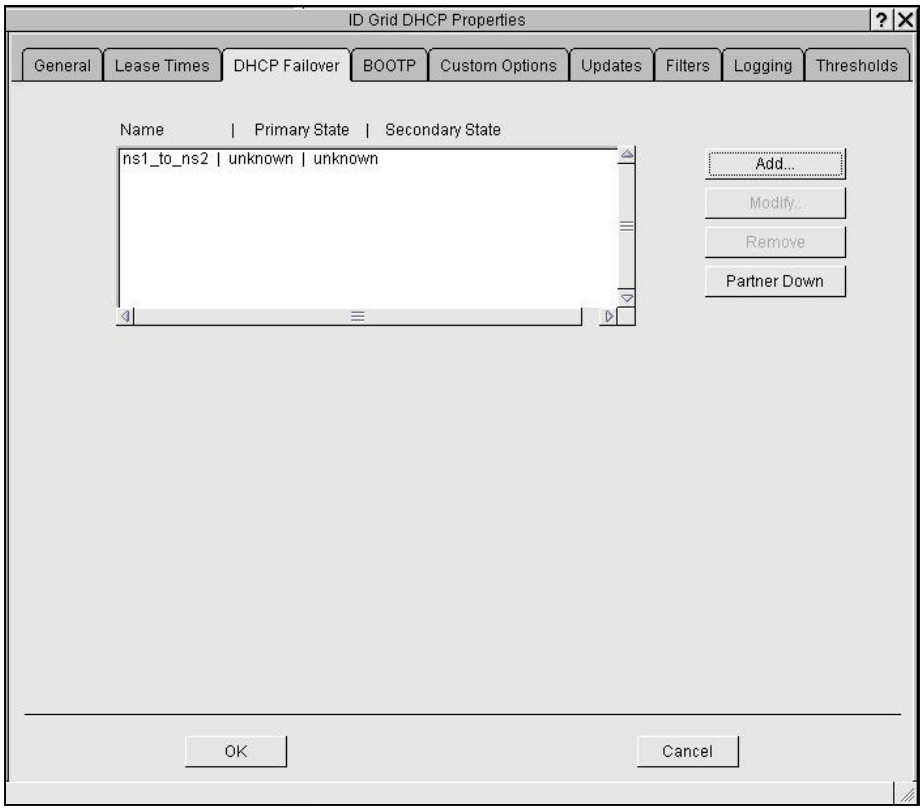
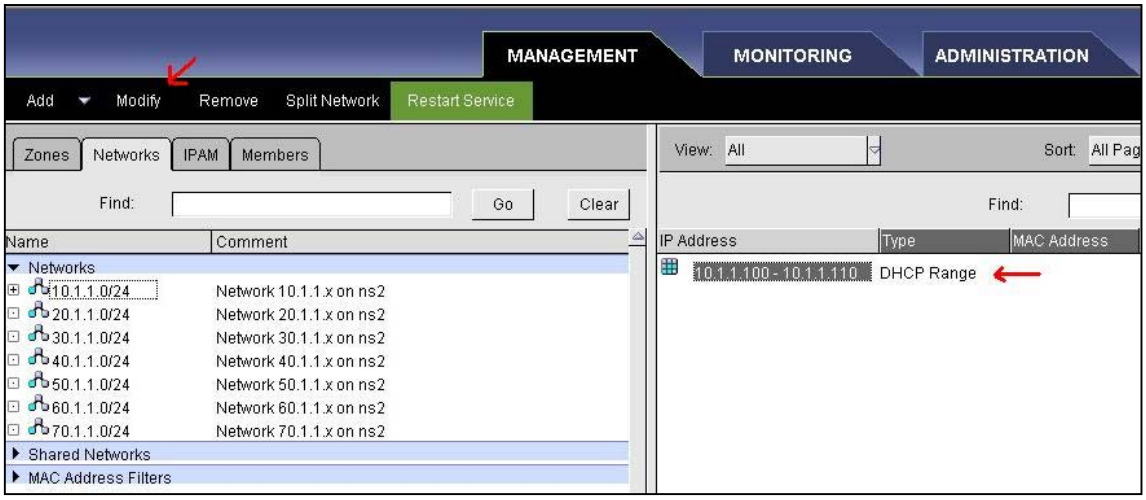
©2006 Avaya Inc. All Rights Reserved.

Step	Description
4.	In the Members page that appears, browse to **ID Grid → Infoblox** in the left hand pane, click or highlight the **DHCP** (ID Grid DHCP Properties) service on the right hand pane, then click **Modify** in the menu bar located above the Members tab.
5.	In the ID Grid DHCP Properties popup that appears, select the **DHCP Failover** tab. 

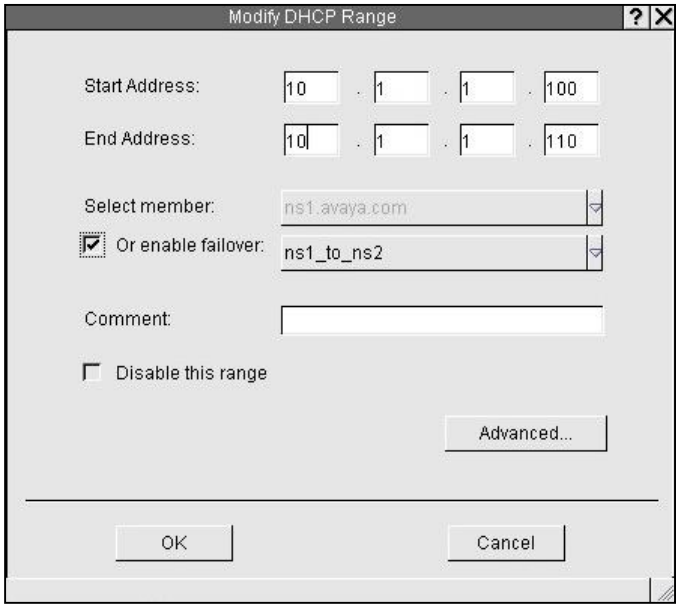
©2006 Avaya Inc. All Rights Reserved.

Step	Description
6.	In the DHCP Failover tab that appears, click **Add…** 
7.	In the Add Failover Association popup that appears, set **Name of Association** to the same name used for the Association in Section 5.1.1 Step 7, check **External Primary** and enter the IP address of the Primary DNSone for External Primary. Click **OK**. 

©2006 Avaya Inc. All Rights Reserved.

Step	Description
8.	In the DHCP Failover tab, click **OK**. 
9.	In the Members page that appears, select the **Networks** tab (not shown).
10.	In the Networks page that appears, browse to **Networks → 10.1.1.0/24** in the left hand pane, click or highlight the **10.1.1.100 – 10.1.1.110** (DHCP Range) on the right hand pane then click **Modify** in the menu bar located above the Members tab. 

©2006 Avaya Inc. All Rights Reserved.

Step	Description
11.	In the Modify DHCP Range popup that appears, check **Or enable failover** and set the pull down list next to the field to the name set for ***Name of Association*** in Step 7. Click **OK**. 
12.	Repeat Steps 10 – 11 for each VLAN defined in **Table 1**. For the purposes of these Application Notes, all VLANs in **Table 1** were modified.
13.	Click **Restart Service** (not shown).
14.	In the Restart Service popup that appears, select **Immediately** and click **OK**. This completes configuration of the Secondary DNSone for DHCP Failover.

©2006 Avaya Inc. All Rights Reserved.

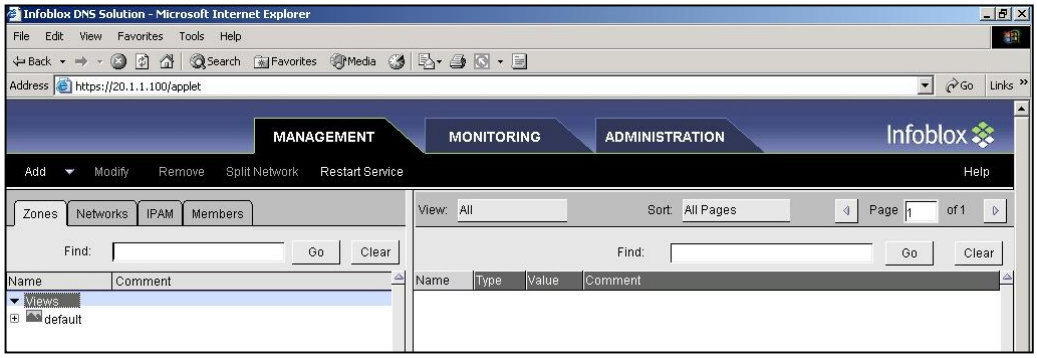
5.2. Configure High Availability

The instructions in this section assume:

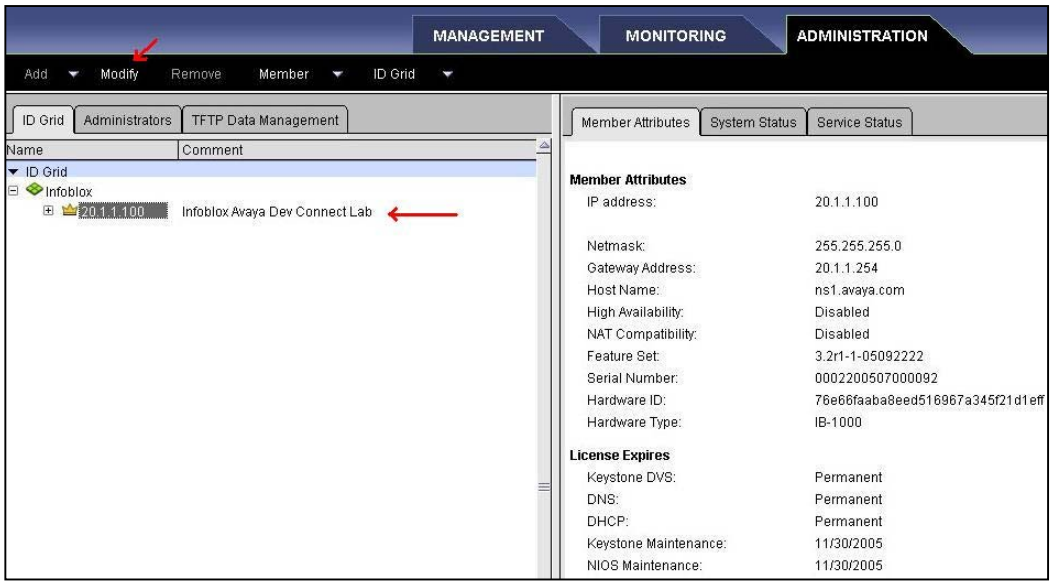
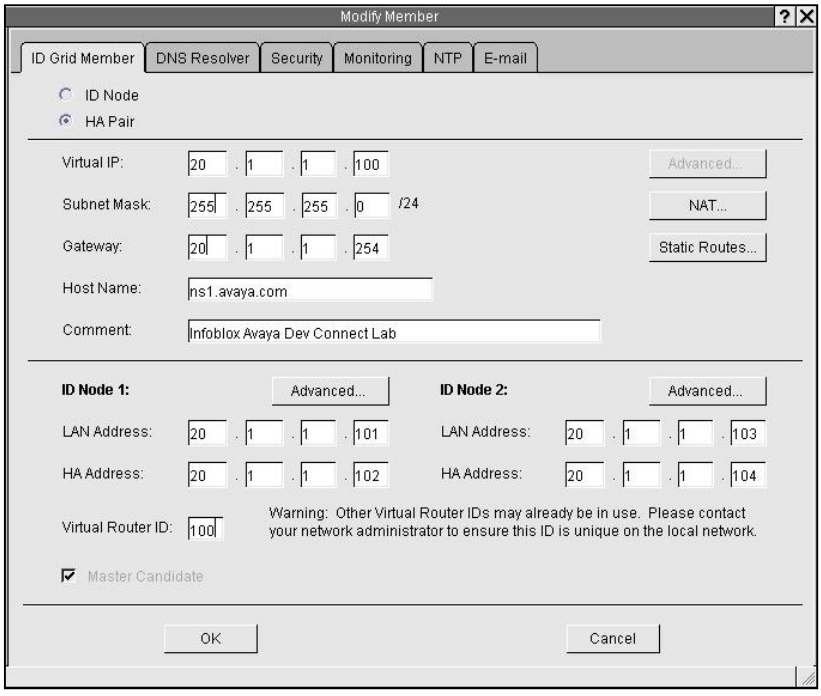
- DNSone ID Node 1 (active node) in **Figure 2** has initially been configured with network IP address, 20.1.1.100, via the console port.
- DNSone ID Node 2 (passive node) in **Figure 2** has initially been configured with network IP address, 20.1.1.103, via the console port.
- DNSone ID Node 1 in **Figure 2** has been configured as per instructions provided in Sections 5.1 – 5.3 of the *Application Notes for Infoblox DNSone in an Avaya Communication Manager IP Telephony Infrastructure* in reference [4].

The *20.1.1.100* IP address assigned to *DNSone ID Node 1* will become the Virtual IP address of the High Availability configuration in the steps that follow. The *DNSone ID Node 1* will then be assigned a different IP address.

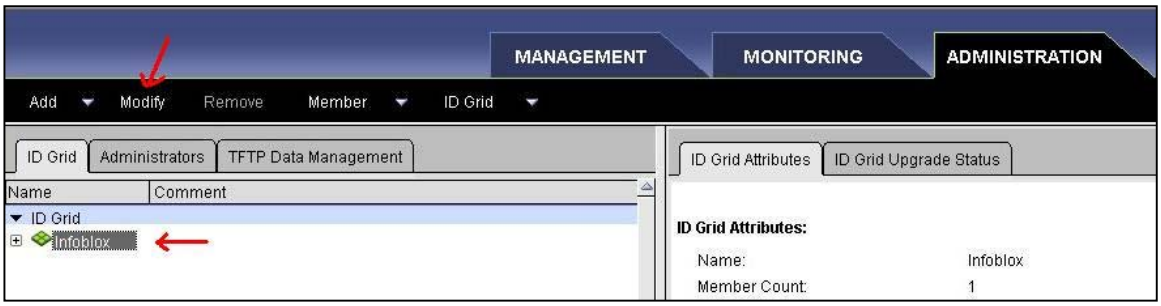
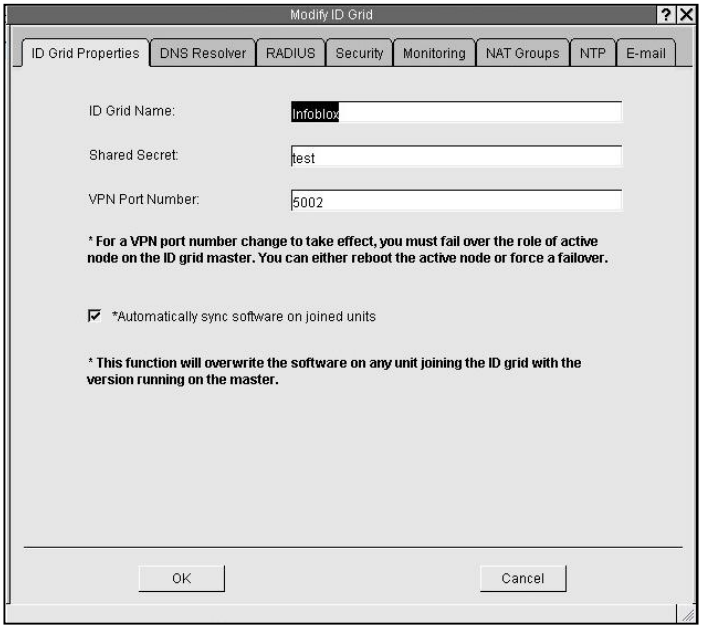
5.2.1. Configure DNSone ID Node 1 (active node)

Step	Description
1.	From a computer in the network, launch a browser and browse to https://20.1.1.100. Log into the Infoblox DNSone with the appropriate credentials (not shown).
2.	If a Warning – HTTPS popup (not shown) appears, click **Yes**.
3.	In the Infoblox DNS Solution page that appears, select the **ADMINISTRATION** tab in the top right of the window.  Infoblox DNS Solution - Microsoft Internet Explorer File Edit View Favorites Tools Help Address https://20.1.1.100/applet MANAGEMENT MONITORING ADMINISTRATION Infoblox Add Modify Remove Split Network Restart Service Help Zones Networks IPAM Members Find: Go Clear Name Comment Views default View: All Sort: All Pages Page 1 of 1 Find: Go Clear Name Type Value Comment

©2006 Avaya Inc. All Rights Reserved.

Step	Description
4.	In the page that appears, browse to **ID Grid → Infoblox → 20.1.1.100** in the left hand pane then click **Modify** in the menu bar located above the ID Grid tab. 
5.	In the Modify Member popup that appears, select **HA Pair**, set **Virtual IP** to ***20.1.1.100***, **Subnet Mask** to ***255.255.255.0***, and **Gateway** to ***20.1.1.254***. In **ID Node 1**, set **LAN Address** and **HA Address** to the IP addresses defined for **ID Node 1** in **Figure 2**. In **ID Node 2**, set **LAN Address** and **HA Address** to the IP addresses defined for **ID Node 2** in **Figure 2** and set **Virtual Router ID** to a unique number. Click **OK**. 

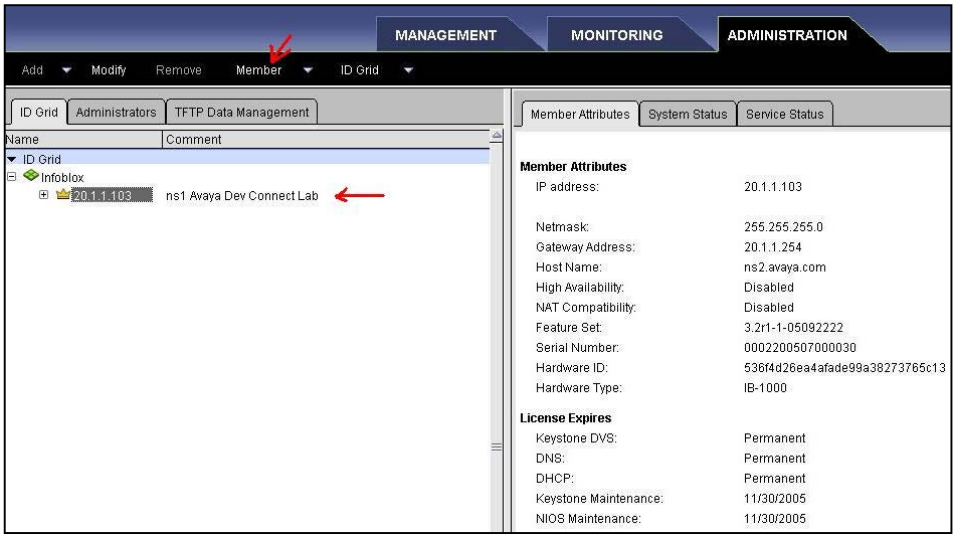
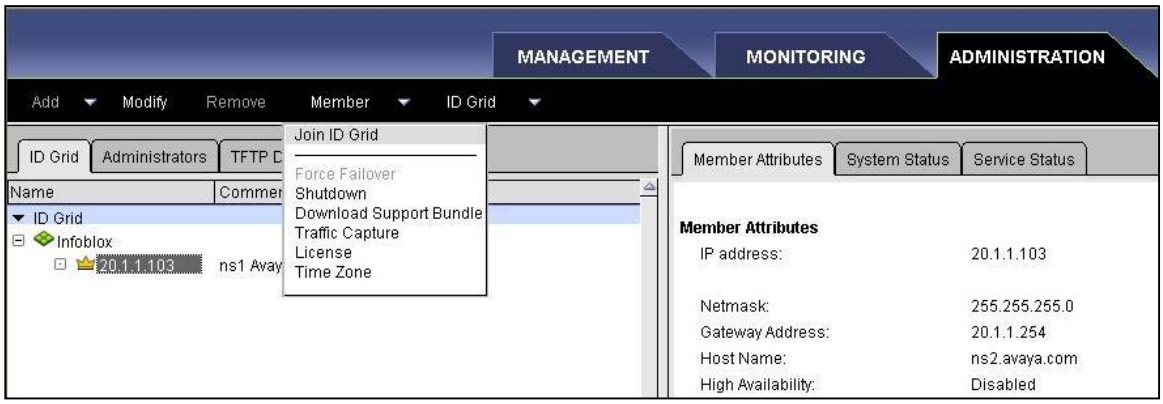
©2006 Avaya Inc. All Rights Reserved.

Step	Description
6.	In the page that appears, browse to **ID Grid → Infoblox** in the left hand pane, then click **Modify** in the menu bar located above the ID Grid tab. 
7.	In the Modify ID Grid popup that appears, set **ID Grid Name** to the name of the grid, **Shared Secret** to a shared secret value to be used and click **OK**. This completes configuration of DNSone ID Node 1 for High Availability. 

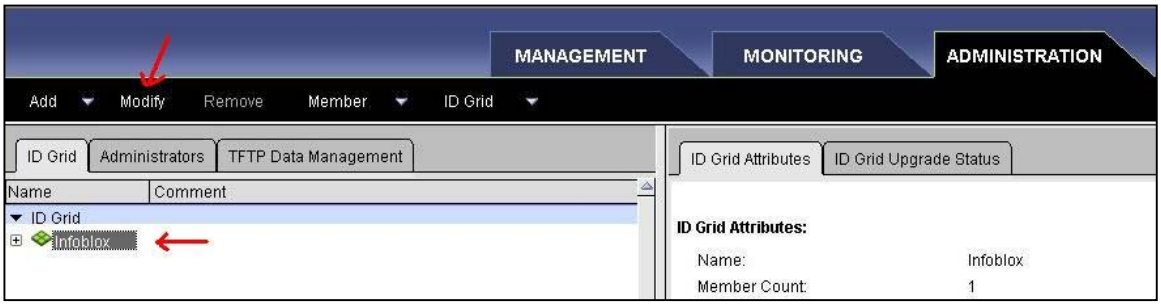
5.2.2. Configure DNSone ID Node 2 (passive node)

Step	Description
1.	From a computer in the network, launch a browser and browse to https://20.1.1.103. Log into the Infoblox DNSone with the appropriate credentials (not shown).
2.	If a Warning – HTTPS popup (not shown) appears, click **Yes**.
3.	In the Infoblox DNS Solution page that appears, select the **ADMINISTRATION** tab in the top right of the window (not shown).

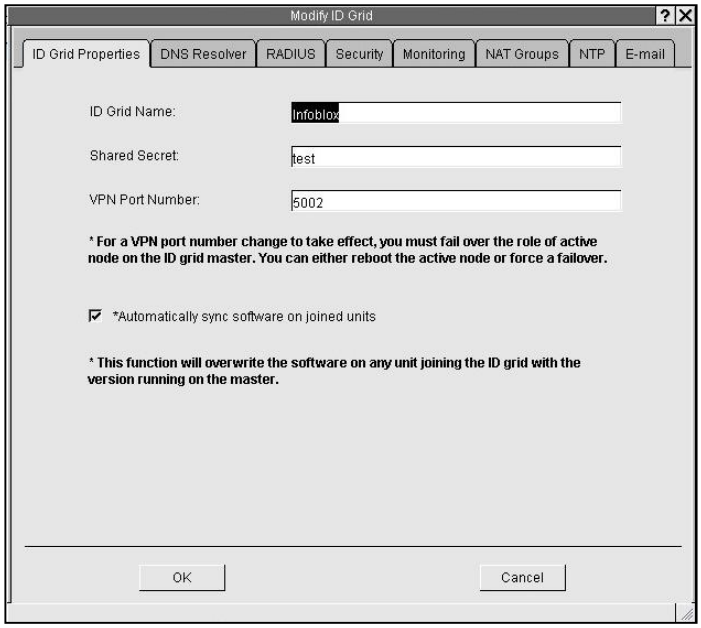
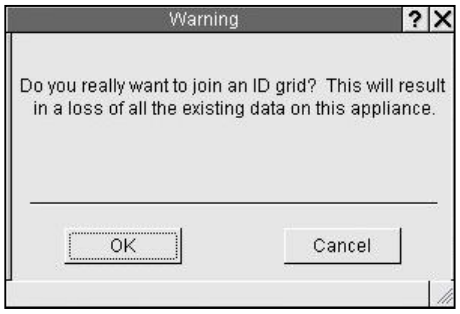
©2006 Avaya Inc. All Rights Reserved.

Step	Description
4.	In the page that appears, browse to **ID Grid → Infoblox → 20.1.1.103** in the left hand pane then click **Member** in the menu bar located above the ID Grid tab. 
5.	Select **Join ID Grid** in the popup menu that appears. 

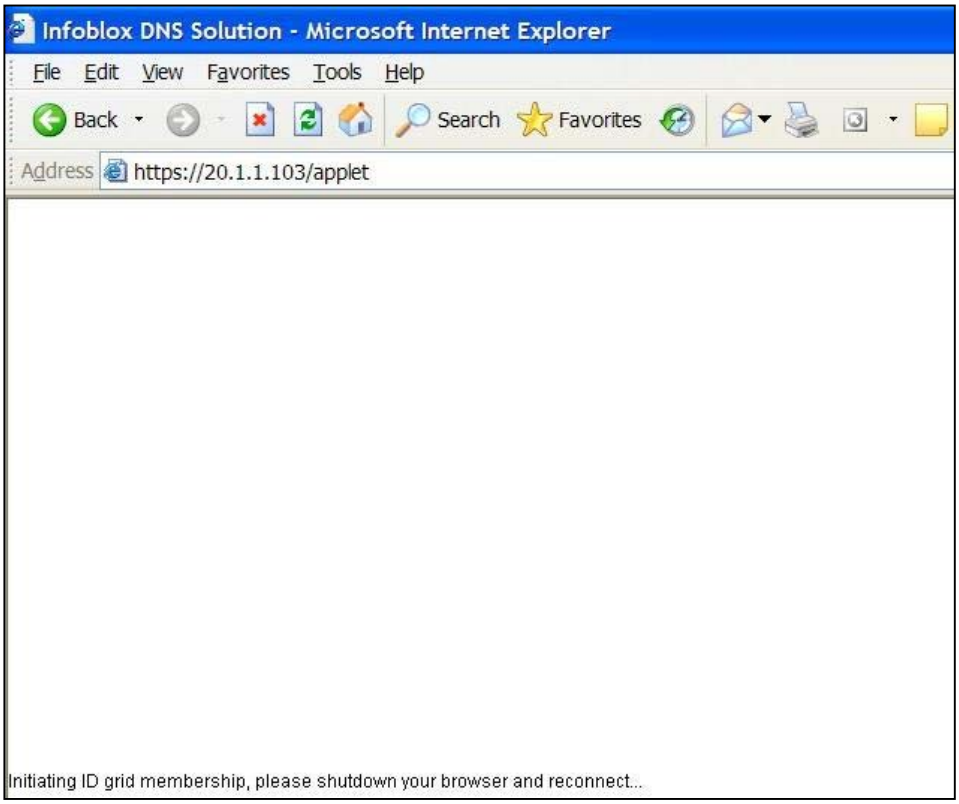
©2006 Avaya Inc. All Rights Reserved.

Step	Description
6.	In the Join ID Grid popup that appears, set **Master's Virtual IP** to the virtual IP address of the HA Pair as depicted in **Figure 2** and defined in **Virtual IP** in Section 5.2.1 Step 6, set **ID Grid Name** to the name of the grid defined in Section 5.2.1 Step 8, set **Shared Secret** to the same value defined for the shared secret in Section 5.2.1 Step 8. Click **OK**.
7.	In the page that appears, browse to **ID Grid → Infoblox** in the left hand pane then click **Modify** in the menu bar located above the ID Grid tab. 

©2006 Avaya Inc. All Rights Reserved.

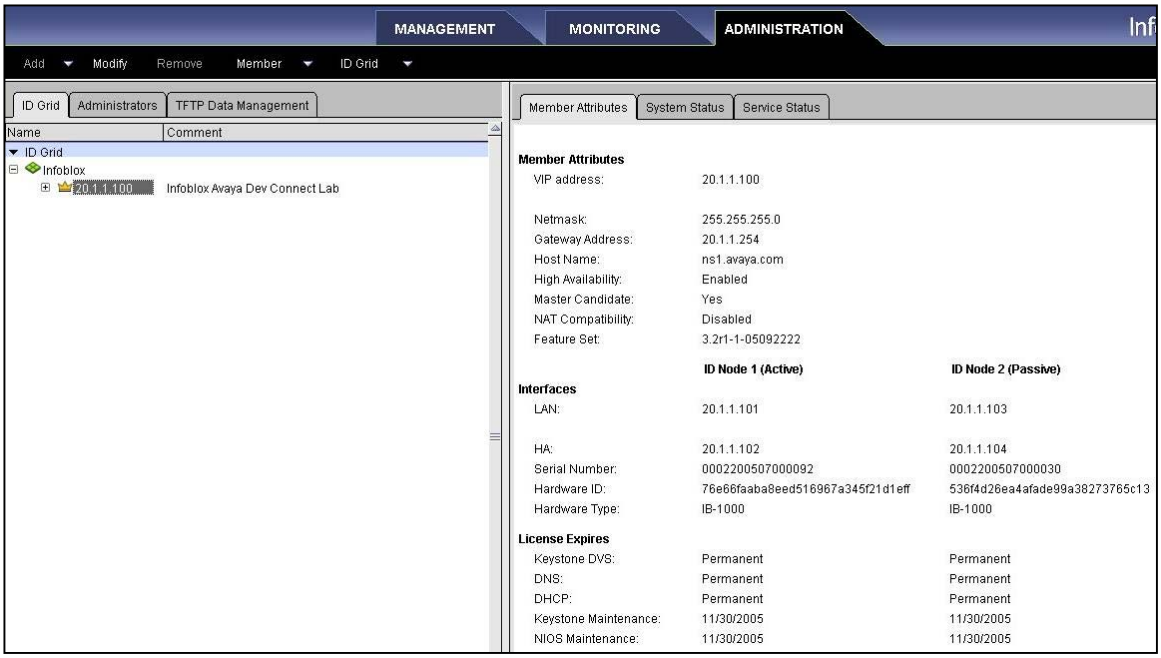
Step	Description
8.	In the Modify ID Grid popup that appears, set **Shared Secret** to a shared secret value to be used and click **OK**. 
9.	In the Warning popup that appears, click **OK**. 

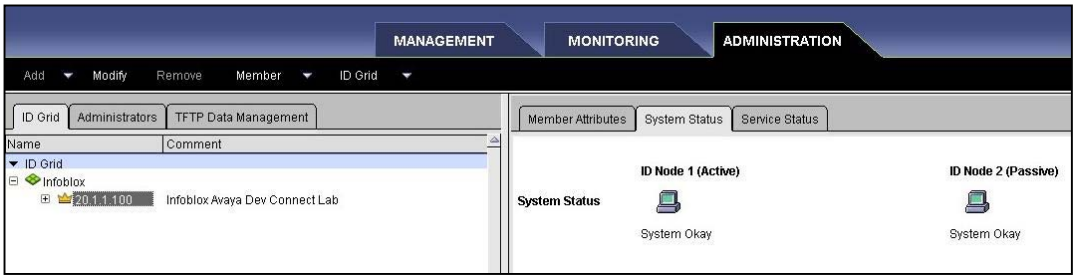
©2006 Avaya Inc. All Rights Reserved.

Step	Description
10.	The message 'Initiating ID grid membership, please shutdown your browser and reconnect…' appears in the browser. This completes configuration of DNSone ID Node 2 for High Availability. 
	The information that follows is provided for informational purposes
11.	From a computer in the network, launch a browser and browse to https://20.1.1.100. Log into the Infoblox DNSone with the appropriate credentials (not shown).
12.	If a Warning – HTTPS popup (not shown) appears, click **Yes**.
13.	In the Infoblox DNS Solution page that appears, select the **ADMINISTRATION** tab in the top right of the window (not shown).

©2006 Avaya Inc. All Rights Reserved.

Step	Description
14.	In the page that appears, browse to **ID Grid → Infoblox → 20.1.1.100** in the left hand pane then select the Member Attributes tab in the right hand pane. The page that appears in the right hand pane shows the High Availability configuration details.
15.	In the right hand pane, click the System Status tab. The page that appears in the right hand pane shows which node is active and which one is passive.





6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the Infoblox DNSone properly provided DHCP and TFTP services for Avaya 4600 Series IP Telephones in an Avaya Communication Manager IP Telephony Infrastructure when configured for DHCP Failover as well as when configured for High Availability.

©2006 Avaya Inc. All Rights Reserved.

6.1. General Test Approach

The general test approach was to verify that the Avaya 4600 Series IP Telephones successfully receive responses to DHCP and TFTP requests from the Infoblox DNSone in DHCP Failover and High Availability scenarios.

6.2. Test Results

All executed test cases completed successfully with the observation noted below:

- **TFTP Failover does not apply to the DHCP Failover configuration (i.e., the Figure 1 network, using the Table 1 DHCP options)** – If the Primary DNSone is also configured as the TFTP server for the solution, when it becomes unavailable, the Secondary DNSone will assume its DHCP responsibilities, not its TFTP responsibilities. Although not used in this compliance test configuration, note that Avaya 4600 Series IP Telephones support a comma-separated list of TFTP servers in the TFTPSRVR parameter for Option 176. Please refer to [1] for information on how to configure the TFTPSRVR parameter with more than one TFTP server.

7. Verification Steps

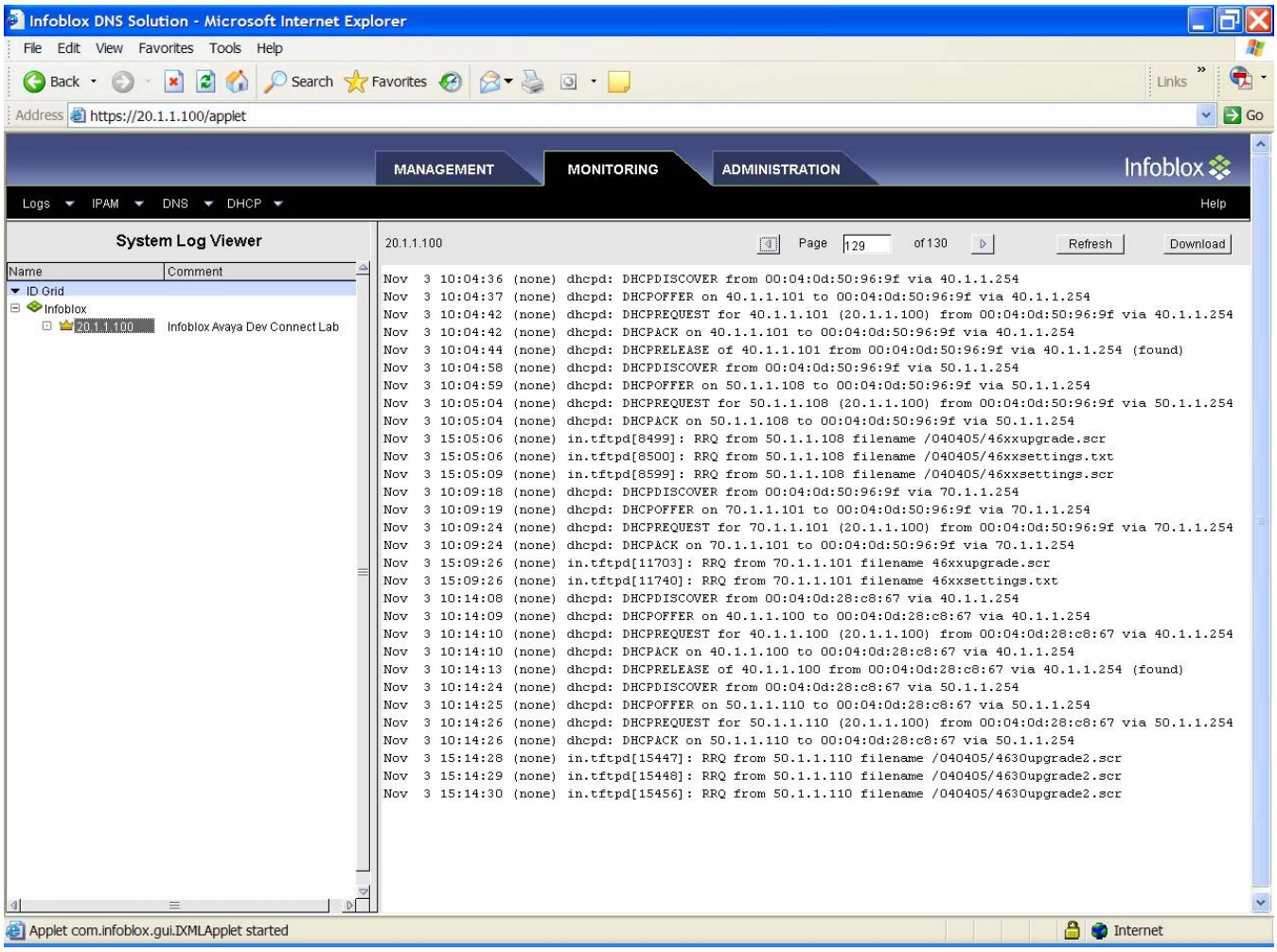
The following steps may be used to verify the configuration between the DNSone and the Avaya 4600 IP Telephones in an Avaya Communication Manager IP network.

- DHCP Failover:
    - Disconnect the Primary DNSone from the network. Verify the Secondary DNSone renews all IP address leases when DHCP leases expire.
    - Power cycle one of the Avaya 4600 IP Telephones in the configuration and verify the Secondary DNSone provides the correct DHCP information.
    - Reset one of the Avaya 4600 IP Telephones in the configuration to factory defaults and verify the Secondary DNSone provides the correct DHCP information.

- High Availability:
    - Disconnect the ID Node 1 DNSone from the network. Verify ID Node 2 DNSone becomes the active node – Section 5.2.2 Steps 14 – 15.
    - Power cycle one of the Avaya 4600 IP Telephones in the configuration and verify the active DNSone provides the correct DHCP and TFTP information.
    - Reset one of the Avaya 4600 IP Telephones in the configuration to factory defaults and verify the active DNSone provides the correct DHCP and TFTP information.

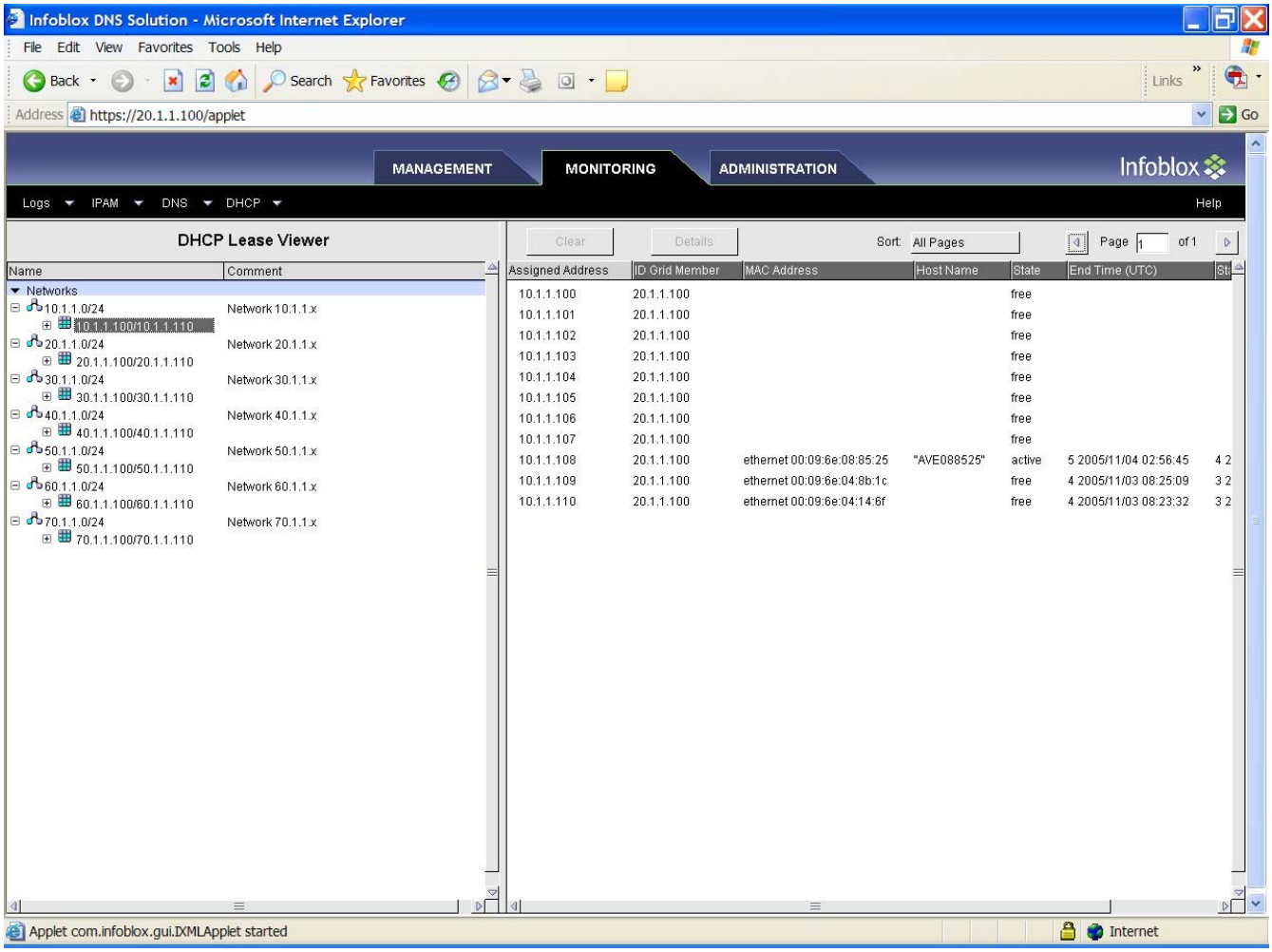
©2006 Avaya Inc. All Rights Reserved.

- To view all DHCP log messages on the DNSone, select the **MONITORING** tab at the top of the page. In the left hand pane, browse to **ID Grid → Infoblox → 20.1.1.100**.


Infoblox DNS Solution - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://20.1.1.100/applet
MANAGEMENT
MONITORING
ADMINISTRATION
Infoblox
Logs IPAM DNS DHCP
Help
System Log Viewer
Name
Comment
ID Grid
Infoblox
20.1.1.100
Infoblox Avaya Dev Connect Lab
20.1.1.100
Page 129 of 130
Refresh
Download
Nov 3 10:04:36 (none) dhcpd: DHCPDISCOVER from 00:04:0d:50:96:9f via 40.1.1.254
Nov 3 10:04:37 (none) dhcpd: DHCPOFFER on 40.1.1.101 to 00:04:0d:50:96:9f via 40.1.1.254
Nov 3 10:04:42 (none) dhcpd: DHCPREQUEST for 40.1.1.101 (20.1.1.100) from 00:04:0d:50:96:9f via 40.1.1.254
Nov 3 10:04:42 (none) dhcpd: DHCPACK on 40.1.1.101 to 00:04:0d:50:96:9f via 40.1.1.254
Nov 3 10:04:44 (none) dhcpd: DHCPRELEASE of 40.1.1.101 from 00:04:0d:50:96:9f via 40.1.1.254 (found)
Nov 3 10:04:58 (none) dhcpd: DHCPDISCOVER from 00:04:0d:50:96:9f via 50.1.1.254
Nov 3 10:04:59 (none) dhcpd: DHCPOFFER on 50.1.1.108 to 00:04:0d:50:96:9f via 50.1.1.254
Nov 3 10:05:04 (none) dhcpd: DHCPREQUEST for 50.1.1.108 (20.1.1.100) from 00:04:0d:50:96:9f via 50.1.1.254
Nov 3 10:05:04 (none) dhcpd: DHCPACK on 50.1.1.108 to 00:04:0d:50:96:9f via 50.1.1.254
Nov 3 15:05:06 (none) in.tftpd[8499]: RRQ from 50.1.1.108 filename /040405/46xxupgrade.scr
Nov 3 15:05:06 (none) in.tftpd[8500]: RRQ from 50.1.1.108 filename /040405/46xxsettings.txt
Nov 3 15:05:09 (none) in.tftpd[8599]: RRQ from 50.1.1.108 filename /040405/46xxsettings.scr
Nov 3 10:09:18 (none) dhcpd: DHCPDISCOVER from 00:04:0d:50:96:9f via 70.1.1.254
Nov 3 10:09:19 (none) dhcpd: DHCPOFFER on 70.1.1.101 to 00:04:0d:50:96:9f via 70.1.1.254
Nov 3 10:09:24 (none) dhcpd: DHCPREQUEST for 70.1.1.101 (20.1.1.100) from 00:04:0d:50:96:9f via 70.1.1.254
Nov 3 10:09:24 (none) dhcpd: DHCPACK on 70.1.1.101 to 00:04:0d:50:96:9f via 70.1.1.254
Nov 3 15:09:26 (none) in.tftpd[11703]: RRQ from 70.1.1.101 filename 46xxupgrade.scr
Nov 3 15:09:26 (none) in.tftpd[11740]: RRQ from 70.1.1.101 filename 46xxsettings.txt
Nov 3 10:14:08 (none) dhcpd: DHCPDISCOVER from 00:04:0d:28:c8:67 via 40.1.1.254
Nov 3 10:14:09 (none) dhcpd: DHCPOFFER on 40.1.1.100 to 00:04:0d:28:c8:67 via 40.1.1.254
Nov 3 10:14:10 (none) dhcpd: DHCPREQUEST for 40.1.1.100 (20.1.1.100) from 00:04:0d:28:c8:67 via 40.1.1.254
Nov 3 10:14:10 (none) dhcpd: DHCPACK on 40.1.1.100 to 00:04:0d:28:c8:67 via 40.1.1.254
Nov 3 10:14:13 (none) dhcpd: DHCPRELEASE of 40.1.1.100 from 00:04:0d:28:c8:67 via 40.1.1.254 (found)
Nov 3 10:14:24 (none) dhcpd: DHCPDISCOVER from 00:04:0d:28:c8:67 via 50.1.1.254
Nov 3 10:14:25 (none) dhcpd: DHCPOFFER on 50.1.1.110 to 00:04:0d:28:c8:67 via 50.1.1.254
Nov 3 10:14:26 (none) dhcpd: DHCPREQUEST for 50.1.1.110 (20.1.1.100) from 00:04:0d:28:c8:67 via 50.1.1.254
Nov 3 10:14:26 (none) dhcpd: DHCPACK on 50.1.1.110 to 00:04:0d:28:c8:67 via 50.1.1.254
Nov 3 15:14:28 (none) in.tftpd[15447]: RRQ from 50.1.1.110 filename /040405/4630upgrade2.scr
Nov 3 15:14:29 (none) in.tftpd[15448]: RRQ from 50.1.1.110 filename /040405/4630upgrade2.scr
Nov 3 15:14:30 (none) in.tftpd[15456]: RRQ from 50.1.1.110 filename /040405/4630upgrade2.scr
Applet com.infoblox.gui.IXMLApplet started
Internet

©2006 Avaya Inc. All Rights Reserved.

- To verify leased IP addresses on the DNSone, select the **MONITORING** tab at the top of the page then click **DHCP** in the menu bar under the MONITORING tab.



8. Support

For technical support on Infoblox products, consult the Infoblox Support Center (ID and password required) at http://www.infoblox.com/support or contact the Infoblox Technical Support at:

- Phone: 888-463-6259 or 408-716-4300, ext. 1
- E-mail: support@infoblox.com

9. Conclusion

These Application Notes describe the steps for configuring the Infoblox DNSone DHCP Failover or High Availability in an Avaya Communication Manager IP Telephony Infrastructure.

©2006 Avaya Inc. All Rights Reserved.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] 4600 Series IP Telephone R2.3 LAN Administrator Guide, 555-233-507, November 2005.

[2] Installation and Configuration Guide Avaya C360 Converged Stackable Switch Software Version 4.3, Issue 1, May 2004.

[3] Reference Guide Avaya C360 Converged Stackable Switch Software Version 4.3, Issue 1, May 2004.

[4] Application Notes for Infoblox DNSone in an Avaya Communication Manager IP Telephony Infrastructure, Issue 1.0, March 2006

[5] Application Notes for Infoblox DNSone in an Avaya IP Office IP Telephony Infrastructure, Issue 1.0, March 2006.

[6] Application Notes for Infoblox DNSone in an Avaya Communication Manager Wireless IP Telephony Infrastructure, Issue 1.0, April 2006.

Product documentation for Infoblox products may be found at http://www.infoblox.com.

[7] DNSone 3.2 Administrator Guide, 2005.

©2006 Avaya Inc. All Rights Reserved.

©2006 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.

©2006 Avaya Inc. All Rights Reserved.